

明細書

ネットワークセキュリティシステム

技術分野

本発明は、ネットワークを通じてデータの送受信をする内部システムを、ネットワークから保護するネットワークセキュリティシステムに関する。

背景技術

インターネット等のネットワークを利用して商品の販売等を行うシステムでは、ネットワークを通じて受注情報を取得し、この受注情報をデータベースに書き込んで、商品の手配や発送等の管理を行っている。このようなシステムでは、万一、ネットワークから不正なデータを取り込んで受注情報が破壊されると、受注活動が停止して重大な被害が発生する。また、万一、不正な手段でネットワークを通じて顧客情報が読みだされると、深刻な信用上の問題が発生する。そこで、いわゆるファイヤーウォールと呼ばれる保護システムをネットワークと内部システムとの間に設けることによって、ハッカー等の侵入を阻止するようにしている。

ところで、上記のような従来技術には、次のような解決すべき課題があった。ファイヤーウォールは、ネットワークを通じて内部システムにアクセスしようとする相手方のアクセス権を確認するために、識別情報や暗証コードなどを要求し、その認証を行なう(特開平11-298639号公報、特開平10-214304号公報)。ところが、不正な手段で識別情報や暗証コードを入手して偽装するハッカーに対する防御は容易でない。しかも、商品の受注販売システムのように、不特定多数のユーザから受注情報を受け入れてこれをデータベースに取り込むものでは、受注情報に混じって侵入する不正なデータを的確に排除する機構が要求される。また、データベースの内容を不正に読みだす行為を的確に排除する機構が要求される。

発明の開示

本発明は以上の点を解決するため次の構成を採用する。

2

〈構成1〉

ネットワークに接続されたサーバと、上記ネットワークを通じてサーバが受信した外部形式のデータを記憶する受信データ記憶手段と、この受信データ記憶手段に記憶された外部形式のデータを、内部形式のデータに変換して、受信処理データ記憶手段に記憶させる受信データ形式変換手段と、上記受信処理データ記憶手段に記憶された内部形式のデータを利用して所定の処理を実行するホストコンピュータとを備えたことを特徴とするネットワークセキュリティシステム。

サーバはネットワークに接続されている。外部形式のデータはネットワークを通じて他の端末装置等から受信される。外部形式のデータのデータ形式は任意でよい。内部形式のデータのデータ形式も任意である。受信データ形式変換手段は、受信データ記憶手段から外部形式のデータを読み取って、所定の手順で内部形式のデータに変換した後、受信処理データ記憶手段に書き込む。受信処理データ記憶手段に記憶された内部形式のデータはホストコンピュータに利用される。受信データ形式変換手段は、外部形式のデータから必要なデータのみを抽出加工して、予め定めた安全な内部形式のデータに変換をする役割を持つ。

ネットワークを通じて受信した外部形式のデータは受信データ記憶手段に書き込まれるが、ホストコンピュータはこの受信データ記憶手段を直接アクセスしない。故に、不正なデータの取り込みが防止できる。即ち、受信データ形式変換手段が外部形式のデータを内部形式のデータに変換する際に、外部形式のデータを安全な内部形式のデータに変換することができるので、不正なデータを排除できる。ホストコンピュータは、任意のタイミングで受信処理データ記憶手段をアクセスして、内部形式のデータを利用すればよい。

〈構成2〉

構成1に記載のネットワークセキュリティシステムにおいて、受信データ記憶手段は、サーバが受信した外部形式のデータの書き込みを許容し、かつ、サーバによるデータの読み出しを禁止し、受信処理データ記憶手段は、ホストコンピュータによる内部形式のデータの読み出しを許容し、かつ、ホストコンピュータによるデータの書き込みを禁止することを特徴とするネットワークセキュリティシステム。

3

受信データ記憶手段がサーバによるデータの読み出しを禁止するのは、ネットワーク側から受信データ記憶手段中のデータの読み出しがされるのを防止するためである。ホストコンピュータによる受信処理データ記憶手段へのデータの書き込みを禁止するのは、ホストコンピュータ側から不用意にデータがネットワーク側へ出力されるのを防止するためである。これにより、ホストコンピュータ側からネットワーク側へのデータの流れが禁止されて、ホストコンピュータ側のデータがネットワーク側に読み出されることが無い。なお、書き込みや読み出しを禁止されるのは全てのデータが対象になり、内部形式のデータも外部形式のデータも別の形式のデータも含む。

〈構成3〉

構成1または2に記載のネットワークセキュリティシステムにおいて、受信データ記憶手段は、受信データ形式変換手段による外部形式のデータの読み出しを許容し、かつ、受信データ形式変換手段によるデータの書き込みを禁止し、受信処理データ記憶手段は、受信データ形式変換手段による内部形式のデータの書き込みを許容し、かつ、受信データ形式変換手段によるデータの読み出しを禁止することを特徴とするネットワークセキュリティシステム。

受信データ形式変換手段は、受信データ記憶手段から外部形式のデータの読み出しのみが許容され、受信処理データ記憶手段への内部形式のデータの書き込みのみが許容される。こうして、受信データ形式変換手段によるデータの流れを、ネットワーク側からホストコンピュータ側への一方通行にしている。これにより、ホストコンピュータ側からネットワーク側へのデータの流れを禁止して、ホストコンピュータ側のデータを保護できる。

〈構成4〉

構成1乃至3のいずれかに記載のネットワークセキュリティシステムにおいて、上記内部形式のデータは、受信処理データ記憶手段からホストコンピュータ側のデータベースに所定のタイミングで追加記憶されることを特徴とするネットワークセキュリティシステム。

受信処理データ記憶手段がホストコンピュータとは別に設けられている場合には、受信処理データ記憶手段からホストコンピュータ側のデータベースに該当す

4

るデータが転送される。受信データ形式変換手段の動作等とは独立した所定のタイミングでデータを転送することができる。ホストコンピュータ側のデータベースのアップデートのタイミングは任意である。

〈構成5〉

構成4に記載のネットワークセキュリティシステムにおいて、上記受信データ形式変換手段による外部形式のデータから内部形式のデータへの変換処理と、上記内部形式のデータのホストコンピュータ側のデータベースへの追加記憶処理はそれぞれ独自のタイミングで一括して実行されることを特徴とするネットワークセキュリティシステム。

サーバが受信データ記憶手段に受信データを書き込むのは、通常、1個のデータごとになる。しかし、受信データ形式変換手段は、変換処理を一括して実行する。一括して実行するというのは、1個のデータごとではなく、バッチ処理のように複数のデータをまとめて処理するという意味である。独自のタイミングで実行されるというのは、それぞれ起動制御が独立しているという意味である。もちろん、例えば、受信データ形式変換手段の変換処理が終了すると自動的に、ホストコンピュータ側のデータベースへの追加記憶処理が開始するように、動作タイミングを制御してもかまわない。

〈構成6〉

構成1乃至3のいずれかに記載のネットワークセキュリティシステムにおいて、受信データ形式変換手段は、外部形式のデータをデータベース形式のデータに変換することを特徴とするネットワークセキュリティシステム。

ネットワークから受信したデータをホストコンピュータで処理するデータベースに取り込むために、必要な変換処理だけを行う。従って、不正なデータがホストコンピュータ側に取り込まれるのを防止できる。

〈構成7〉

構成1乃至3のいずれかに記載のネットワークセキュリティシステムにおいて、サーバは受信データ記憶手段にメール形式のデータを送信して外部形式のデータを書き込むことを特徴とするネットワークセキュリティシステム。

5

サーバが一般の記憶装置上の記憶領域をアクセスして外部形式のデータを書き込むようにするよりも、サーバから受信データ記憶手段にメール形式のデータを送信するようにしたほうが、サーバから受信データ記憶手段へのデータの一方通行性が確保される。

〈構成8〉

構成1乃至3のいずれかに記載のネットワークセキュリティシステムにおいて、上記ネットワークはインターネットであることを特徴とするネットワークセキュリティシステム。

イントラネットに比べてはるかに高いセキュリティが要求されるからこのシステムを採用した。

〈構成9〉

内部形式のデータを利用して所定の処理を実行するホストコンピュータと、ネットワークに送信される内部形式のデータを記憶する送信処理データ記憶手段と、この送信処理データ記憶手段に記憶された内部形式のデータを外部形式のデータに変換して、送信データ記憶手段に記憶させる送信データ形式変換手段と、上記送信データ記憶手段に記憶された外部形式のデータをネットワークに対して送信するサーバとを備えたことを特徴とするネットワークセキュリティシステム。

サーバはネットワークに接続されている。外部形式のデータはネットワークを通じて他の端末装置等に送信される。外部形式のデータやデータ形式、内部形式のデータやデータ形式、データ形式の変換の内容はデータ受信の場合と変わらない。送信データ形式変換手段は、送信処理データ記憶手段から内部形式のデータを読み取って、所定の手順で外部形式のデータに変換した後、送信データ記憶手段に書き込む。

ホストコンピュータは、任意のタイミングで送信処理データ記憶手段に、送信すべき内部形式のデータを書き込む。サーバによりネットワークを通じて送信される外部形式のデータは、送信データ形式変換手段により送信データ記憶手段に書き込まれる。サーバは、送信処理データ記憶手段を直接アクセスしない。故に、誤って、ホストコンピュータ側の保護すべきデータの送信がされるのを防止できる。

〈橋成10〉

構成 9 に記載のネットワークセキュリティシステムにおいて、送信処理データ記憶手段は、ホストコンピュータによる内部形式のデータの書き込みを許容し、かつ、ホストコンピュータによるデータの読み出しを禁止して、送信データ記憶手段は、サーバが送信する外部形式のデータの読み出しを許容し、かつ、サーバによるデータの書き込みを禁止することを特徴とするネットワークセキュリティシステム。

送信処理データ記憶手段がホストコンピュータによるデータの読み出しを禁止するのは、ネットワーク側から不正なデータが侵入するのを防止するためである。サーバによる送信データ記憶手段へのデータの書き込みを禁止するのも、ネットワーク側から不正なデータが侵入するのを防止するためである。これにより、ホストコンピュータ側からネットワーク側へのデータの流れのみが確保されて、ホストコンピュータを含む内部システムが保護される。なお、書き込みや読み出しを禁止されるのは全てのデータが対象になり、その形式は問わない。

〈構成 1 1〉

構成 9 または 10 に記載のネットワークセキュリティシステムにおいて、送信処理データ記憶手段は、送信データ形式変換手段による内部形式のデータの読み出しを許容し、かつ、送信データ形式変換手段によるデータの書き込みを禁止し、送信データ記憶手段は、送信データ形式変換手段による外部形式のデータの書き込みを許容し、かつ、送信データ形式変換手段によるデータの読み出しを禁止することを特徴とするネットワークセキュリティシステム。

送信データ形式変換手段は、送信処理データ記憶手段から内部形式のデータの読み出しのみが許容され、送信処理データ記憶手段への外部形式のデータの書き込みのみが許容される。こうして、送信データ形式変換手段によるデータの流れを、ホストコンピュータ側からネットワーク側への一方通行にしている。これにより、ネットワーク側からホストコンピュータ側へのデータの流れを禁止して、ホストコンピュータ側のデータを保護できる。

〈構成12〉

構成 0 乃至 11 のいずれかに記載のネットワークセキュリティシステムにおいて、上記送信データ形式変換手段による内部形式のデータから外部形式のデータへの変換処理は、上記ホストコンピュータによる送信処理データ記憶手段への内部形式のデータの記憶処理とは独立したタイミングで実行されることを特徴とするネットワークセキュリティシステム。

送信処理データ記憶手段を設けているので、送信データ形式変換手段は、変換処理を任意のタイミングで実行できる。また、ホストコンピュータも任意のタイミングで送信用の内部形式のデータを送信処理データ記憶手段へ書き込むことができる。送信用の内部データの形式は自由で、データベース用とは限らない。

〈機成13〉

構成 9 乃至 11 のいずれかに記載のネットワークセキュリティシステムにおいて、サーバは送信データ記憶手段からメール形式のデータを受信してネットワークに送信することを特徴とするネットワークセキュリティシステム。

サーバが一般の記憶装置上の記憶領域をアクセスして外部形式のデータを書き込むようにするよりも、サーバが送信データ記憶手段からメール形式のデータを受信するようにしたほうが、送信データ記憶手段からサーバへのデータの一方通行性が確保される。

〈構成14〉

構成 9 乃至 11 のいずれかに記載のネットワークセキュリティシステムにおいて、上記ネットワークはインターネットであることを特徴とするネットワークセキュリティシステム。

イントラネットに比べてはるかに高いセキュリティが要求されるからこのシステムを採用した。

〈構成15〉

ネットワークを通じてサーバが受信した外部形式のデータを記憶する受信データ記憶手段と、この受信データ記憶手段に記憶された外部形式のデータを、内部形式のデータに変換して、受信処理データ記憶手段に記憶させる受信データ形式変換手段と、上記受信処理データ記憶手段に記憶された内部形式のデータを利用して所定の処理を実行するホストコンピュータと、ネットワークに送信される内部

[illegible]

8

形式のデータを記憶する送信処理データ記憶手段と、この送信処理データ記憶手段に記憶された内部形式のデータを外部形式のデータに変換して、送信データ記憶手段に記憶させる送信データ形式変換手段と、上記送信データ記憶手段に記憶された外部形式のデータをネットワークに対して送信するサーバとを備えたことを特徴とするネットワークセキュリティシステム。

構成1のデータ受信機能と構成9のデータ送信機能の双方を備えたシステムである。

〈構成16〉

構成15に記載のネットワークセキュリティシステムにおいて、上記受信データ形式変換手段による外部形式のデータから内部形式のデータへの変換処理と、上記内部形式のデータのホストコンピュータ側のデータベースへの追加記憶処理と、上記送信データ形式変換手段による内部形式のデータから外部形式のデータへの変換処理と、上記ホストコンピュータによる送信処理データ記憶手段への内部形式のデータの記憶処理とは、それぞれ独立したタイミングで実行されることを特徴とするネットワークセキュリティシステム。

このように一方通行の障壁を設け、かつ、それぞれ独自のタイミングで順次データ転送を行うようにしているので、ネットワークからのホストコンピュータ側の保護が強固になる。故に、ネットワーク側から構成1のデータ受信機能を利用して所定のコマンドを送り込み、構成9のデータ送信機能を利用してホストコンピュータ側から何らかのデータを読みだすのは不可能になるという効果がある。

〈構成17〉

ネットワークに接続されたサーバと、ホストコンピュータ側に接続されたメール転送部とから成り、上記サーバにはメールクライアントとメールサーバとが設けられ、上記メール転送部には、上記メールクライアントから通信回線を介してメールを受信するメール受信部と、上記メールサーバに通信回線を介してメールを送信するメール送信部とが設けられ、上記ホストコンピュータは上記メール転送部のメール受信部を介して上記サーバからデータの転送を受け、上記メール転送部のメール送信部を介して上記サーバにデータを転送することを特徴とするネットワークセキュリティシステム。

サーバとメール転送部との間でのデータ転送は、一定のメール形式以外で行われることがない。ホストコンピュータはメール転送部を介してのみ、サーバとデータの授受を行う。故に、不正なコマンドやプログラムがサーバとメール転送部との間で転送されることが無い。

〈構成18〉

構成17に記載のネットワークセキュリティシステムにおいて、上記通信回線は、メール専用の通信回線であることを特徴とするネットワークセキュリティシステム。

メール専用であって、他のデータの侵入経路を持たない通信回線を用いてサーバとメール転送部とを接続すれば、より確実にセキュリティを保つことができる。

〈構成19〉

ネットワークに側に設けたメールサーバと、ホストコンピュータ側に設けられたメール転送部とから成り、上記メール転送部には、上記メールサーバからメール専用線を介してメールを受信するメール受信部と、上記メールサーバにメール専用線を介してメールを送信するメール送信部とが設けられ、上記ホストコンピュータは上記メール転送部のメール受信部を介して上記メールサーバからデータの転送を受け、上記メール転送部のメール送信部を介して上記メールサーバにデータを転送することを特徴とするネットワークセキュリティシステム。

以上の構成においては、ネットワーク側にメールサーバを配置して、このメールサーバとホストコンピュータ側のメール転送部との間のメール送受信を専用線を介して行う。専用線は、通信線であればなんでもよいが、メールサーバとホストコンピュータ側の通信にのみ使用される。専用線により一定の手段によってのみネットワークとホストコンピュータとの間のデータ転送をするので、ホストコンピュータ側がネットワーク側から保護される。

図面の簡単な説明

図1は、本発明のシステムの具体例を示すブロック図である。

図2は、サーバが受信したデータが変換されて受信処理データ記憶手段に記憶されるまでの動作を説明する説明図である

図3は、サーバや受信処理データ記憶手段等の動作のフローチャートである。

図4は、本発明を送信処理のためのシステムに利用した例を示すブロックである。

図5は、セキュリティ機能をさらに強化したシステムのブロック図である。

図6は、メール送信を利用してセキュリティ機能を強化した別システムのブロック図である。

発明を実施するための最良の形態

以下、本発明の実施の形態を具体例を用いて説明する。

(受信処理)

図1は、本発明のシステムの具体例を示すブロック図である。図のように、ネットワーク1にはユーザの利用する様々な端末装置2が接続されている。これらの端末装置2に対して、例えば、商品購入の為の情報を提供するシステムが接続されている。このシステムは、本発明により保護機能を強化したネットワークセキュリティシステム20を構成している。ネットワークセキュリティシステム20は、サーバ3、受信データ記憶手段6、受信データ形式変換手段7、受信処理データ記憶手段8及びホストコンピュータ10を備える。

サーバ3は、ネットワーク1に接続されている。サーバ3の内部には、ユーザに提供するための情報を記憶した図示しない記憶装置が組み込まれている。なお、このネットワークは、インターネットが適するが、この他に、利用者を特定した電話網、イントラネットその他あらゆるネットワークに適用が可能である。

ユーザから商品の受注をしたときには、その受注情報はネットワーク1を通じてサーバ3が受信する。この受注情報を処理して商品の手配や管理を行うために、ホストコンピュータ10が設けられている。受信データ記憶手段6と、受信データ形式変換手段7と、受信処理データ記憶手段8は、サーバが受信した受注情報をホストコンピュータ10に送り込むためのものである。ホストコンピュータ10は、受信処理データ記憶手段8からデータベース記憶部9にその受注情報を受け入れて、受注管理を行う。

受信データ記憶手段6は、ネットワークを通じてサーバ3が受信した外部形式のデータ4を記憶する記憶装置により構成される。外部形式のデータ4はネットワークを通じて他の端末装置等から受信されるもので、Eメール形式、データファイル形式等の任意の形式のデータである。また、テキスト形式のデータでもバイナリ形式のデータでも構わない。受信データ形式変換手段7は、受信データ記憶手段6から外部形式のデータ4を読み取って、所定の手順で内部形式のデータ5に変換した後、受信処理データ記憶手段8に書き込む機能を持つ。受信データ形式変換手段7は、コンピュータプログラムにより実現するとよいが、ハードウェアにより実現することもできる。データ形式の変換は、抽出、並べ替え、部分的な削除、データの追加等、自由に設定できる。受信データ形式変換手段7は、単なるデータの転送をしないので受信データに含まれる不正なデータをフィルタリングする効果がある。

内部形式のデータ5の形式も任意であるが、予めホストコンピュータ側で規定された所定のフォーマットのデータである。この例では、データベース記憶部9に記憶されたデータベースを容易にアップデートすることができるように、CSV形式のデータとする。このCSV形式のデータは、データが項目毎にカンマやタブで区切られたテキスト形式のデータである。受信データ形式変換手段7は、サーバ3の受信した外部形式のデータを解析して、必要なデータ項目を抽出し、内部形式のデータを生成する。受信処理データ記憶手段8は、この内部形式のデータ5を所定量記憶して、データベース記憶部9にその内部形式のデータ5を書き込む迄保持する記憶装置である。

図2は、サーバが受信したデータが変換されて受信処理データ記憶手段に記憶されるまでの動作を説明する説明図である。また、図3は、サーバや受信処理データ記憶手段等の動作のフローチャートである。

これらの図を用いて、その動作を説明する。まず、サーバは、図1に示したネットワーク1から受信したデータD1を順番に受信データ記憶手段6に書き込む(図3ステップS.1、ステップS.2)。受信データ記憶手段6に蓄積されたデータD2は、所定のタイミングで受信データ形式変換手段7により読み取られ、外

部形式のデータ4から内部形式のデータ5への変換処理が行われる(図3ステップS3、ステップS4)。

例えば、受注データ管理の場合には、こうした変換処理は、毎日夜間に1回とか、1日2回とか、2時間置きといったように設定される。従って、受信データ形式変換手段7はシステムタイマを監視して、変換開始時刻になったときその動作を開始するとよい。受注管理の場合には、ユーザコード、受注商品コード、受注個数、等のデータを含むメール等の形式のデータが受信データ記憶手段に記憶される。外部形式のデータ中に、例えば、ユーザコードの位置を示すデータが含まれていれば、そのデータを検出して切り取り、ユーザコードの部分のみを抽出できる。このとき、ユーザコードやその他の必要なデータ以外の部分は自動的に切り捨てられるので、不正なデータの取り込みが防止される。データ取り込みの際に、そのデータのフォーマットも検査するようにすれば、偽装されたデータの取り込みも防止できる。受信データ形式変換手段7は、こうして必要データ項目を抽出して、例えば、カンマで区切ったテキストデータを生成する。このデータを受信処理データ記憶手段8に書き込む。

受信データ記憶手段に記憶された全てのデータD2の変換処理が終了すると、図3のステップS5からステップS6に進み、データベースのアップデート処理を実行する。受信処理データ記憶手段8に記憶されたデータD3は、そのままデータベースへ追記される。このデータD3が上記のようなCSV形式のデータの場合には、データベースへそのまま取り込むことができ、受注管理に使用される。

なお、上記の例では、受信データ形式変換手段7による外部形式のデータ4から内部形式のデータ5への変換処理を実行してから、続いて、この内部形式のデータ5のホストコンピュータ側のデータベースへの追加記憶処理を実行するようにした。しかしながら、これらの処理はシステムの運用の便宜のために、それぞれ独白に実行されればよい。但し、受信データ形式変換手段7による変換処理は、ある程度外部形式のデータが蓄積されたときや、サーバへのアクセスが集中していないタイミングを狙って実行されることが好ましい。

サーバが受信データ記憶手段に受信データを書き込むのは、通常、1個のデータごとになる。しかし、受信データ形式変換手段は、変換処理を一括して実行す

る。一括して実行するというのは、1個のデータごとではなく、バッチ処理のように複数のデータをまとめて処理するという意味である。独自のタイミングで実行されるというのは、それぞれ起動制御が独立しているという意味である。例えば、受信データ形式変換手段の変換処理が終了すると自動的に、ホストコンピュータ側のデータベースへの追加記憶処理が開始するように、動作タイミングを制御してもかまわない。

受信データ形式変換手段7は、単なるサーバとホストコンピュータとの間のインタフェースではない。不正なデータが含まれているかも知れない外部形式のデータから必要なデータのみを抽出加工して、予め定めた安全な内部形式のデータに変換をする一方通行のフィルタとしての役割を持つ。図1に示したネットワーク1を通じてサーバ3が受信した外部形式のデータは、受信データ記憶手段6に書き込まれるが、ホストコンピュータ10はこの受信データ記憶手段6を直接アクセスしない。故に、ホストコンピュータ10が、ネットワーク1から不正なデータを取り込むのを防止できる。

なお、図 1 において、受信データ記憶手段 6 は、サーバ 3 とは別に独立して設けた記憶装置であっても良いし、サーバやホストコンピュータ 10 の内部に設けられた記憶装置の一部であってもよい。また、受信処理データ記憶手段 8 も、サーバやホストコンピュータ 10 とは別に独立して設けた記憶装置であっても良いし、ホストコンピュータの内部に設けられた記憶装置の一部であってもよい。受信データ形式変換手段 7 は、サーバ 3 上で動作するコンピュータプログラムであってもよいし、ホストコンピュータ 20 上で動作するコンピュータプログラムであってもよい。

さらに、受信データ記憶手段 6 は、サーバ 3 が受信した外部形式のデータの書き込みを許容しても、サーバ 3 によるあらゆるデータの読み出しを禁止することが好ましい。これは、例えば良く知られたオペレーティングシステムの機能により実現する。また、あるいは、後で説明するように、サーバ 3 が受信データ記憶手段 6 にメール形式でデータを転送するようにすればよい。これによりネットワーク 1 側から受信データ記憶手段 6 中のデータの読み出しがされるのを防止できる。また、受信処理データ記憶手段 8 は、ホストコンピュータ 10 による内部形

式のデータの読み出しを許容しても、ホストコンピュータ10によるあらゆるデータの書き込みを禁止することが好ましい。

同様に、受信データ形式変換手段7の動作にも制限を設けることができる。即ち、受信データ記憶手段8は、受信データ形式変換手段7による外部形式のデータの読み出しを許容する一方、受信データ形式変換手段7によるあらゆるデータの書き込みを禁止する。受信処理データ記憶手段8は、受信データ形式変換手段7による内部形式のデータの書き込みを許容する一方、受信データ形式変換手段7によるあらゆるデータの読み出しを禁止する。以上のように、一方通行の障壁をいくつも設けておくことにより、ハッカーから内部システムを有効に保護することが可能になる。

〈送信処理〉

図4は、本発明を送信処理のためのシステムに利用した例を示すブロックである。

図1に示したシステムは、ネットワークを通じて受信したデータを安全にホストコンピュータの処理するデータベース中に取り込むためのものであった。これはホストコンピュータからデータをネットワークに向けて送信する場合にも応用できる。図4はこの例を示すもので、図1のシステムと対比するため、図中に図1のシステムを構成するブロックを破線で表示して区別した。

図4のシステムは、ホストコンピュータ10は、送信データ記憶手段12と、送信データ形式変換手段13と、送信処理データ記憶手段14とを備える。その他は図1のシステムと同様である。ホストコンピュータ10は、データベース記憶部9を使用して、受注管理等を実行する。送信処理データ記憶手段14は、このホストコンピュータが生成してネットワークに送信される、内部形式のデータを記憶する記憶装置である。送信データ形式変換手段13は、送信処理データ記憶手段14に記憶された内部形式のデータを外部形式のデータに変換して、送信データ記憶手段12に記憶させる機能を持つ。これも、図1の例と同様に、コンピュータプログラム等により構成される。サーバ3は、送信データ記憶手段12に記憶された外部形式のデータをネットワークに対して送信する機能を持つ。外部形式のデータ内部形式のデータの内容や形式は図1の例と同様でよい。

このシステムでは、ホストコンピュータ 10 は、ネットワークを通じて送信すべきデータがあると、任意のタイミングでこれを内部形式のデータにして、送信処理データ記憶手段 14 に記憶させる。送信データ形式変換手段 13 は、例えば、ホストコンピュータにより、そのつど起動されて、送信処理データ記憶手段 14 から内部形式のデータを読み取って、外部形式のデータに変換した後、送信データ記憶手段 12 に書き込む。この動作は、図 1 のデータ受信の場合と異なり、ホストコンピュータからデータ送信の緊急性についての情報を取得できるから、その点を考慮して、そのタイミングを選定すればよい。

サーバも、データが送信データ記憶手段 12 に書き込まれた後、データ送信の緊急性を考慮してネットワークへの送信処理を行えば良い。ここで、この例でも、送信処理データ記憶手段 14 は、ホストコンピュータ 10 による内部形式のデータの書き込みを許容する一方、ホストコンピュータ 10 によるデータの読み出しを禁止するとよい。また、送信データ記憶手段 12 は、サーバ 3 が送信する外部形式のデータの読み出しを許容する一方、サーバ 3 によるデータの書き込みを禁止することが好ましい。

さらに、送信処理データ記憶手段 14 は、送信データ形式変換手段 13 による内部形式のデータの読み出しを許容する一方、送信データ形式変換手段 13 によるデータの書き込みを禁止することが好ましい。また、送信データ記憶手段 12 は、送信データ形式変換手段 13 による外部形式のデータの書き込みを許容する一方、送信データ形式変換手段 13 によるデータの読み出しを禁止することが好ましい。以上のようにして、データ送信の場合には、ホストコンピュータからネットワークへの一方通行の障壁をいくつも設けて、ハッカーによるデータの不正取得を防止することができる。

また、送信データ形式変換手段 13 による内部形式のデータから外部形式のデータへの変換処理は、ホストコンピュータ 10 による送信処理データ記憶手段 14 への内部形式のデータの記憶処理とは独立したタイミングで実行してよい。図 1 に示したようなデータ受信のためのシステムと、図 4 に示したようなデータ送信のためのシステムを兼ね備えたシステムは、データの送受信に対して非常に高い保護が可能になる。

このとき、図4に示した受信データ形式変換手段7による変換処理と、内部形式のデータのホストコンピュータ10側のデータベースへの追加記憶処理と、ホストコンピュータ10による送信処理データ記憶手段14へのデータの記憶処理と、送信データ形式変換手段13による変換処理とは、それぞれ独立したタイミングで実行されることが好ましい。

図5は、システムのセキュリティ機能をさらに強化したシステムのブロック図である。

通常、コンピュータの記憶装置については、特定の領域のみを読み出し可能にし、他の領域については読み出しも書き込みも禁止するといった制御が可能である。しかしながら、このような制御はソフトウェアにより行うため、ハッカーによる不正な手段による侵入を完全に防止するのは容易でない。例えば、図1のシステムに示した各機能ブロックを一台のコンピュータを用いて実現した場合には、受信データ記憶手段6と受信処理データ記憶手段8と送信データ記憶手段12と送信処理データ記憶手段14とは同一のメモリ上に割りつけられる場合がある。また、サーバ3とホストコンピュータ10とをLAN（ローカルエリアネットワーク）で直接接続して、記憶装置を共有することもできる。そのような場合、ホストコンピュータ側で保護されるべき受信処理データ記憶手段8や送信処理データ記憶手段14に対する不正アクセスを完全に防ぐのは容易でない。そこで、この例では、サーバとホストコンピュータ側の間を、データの一定形式の転送のみが可能なメールシステムで接続した。

図のサーバ3は、メールクライアント31、記憶装置33、メールサーバ32を備える。また、メール転送部40は、メール受信部41とメール送信部42を備える。更に、データ変換部50は、受信データ記憶手段6と、受信データ形式変換手段7と、受信処理データ記憶手段8と、送信データ記憶手段12とを備える。この具体例では、上記メール転送部40の機能により、サーバ3とホストコンピュータ側のデータ転送形態を制限して、ホストコンピュータ側の保護を強化している。また、メール転送部40に加えて上記データ変換部50を設ければ、より一層システムのセキュリティを高めることができる。

メール転送部40のメール受信部41は、メール受信機能を持つ装置で、メール送信部42はメール送信機能を持つ装置である。このメール転送部40とサーバ3とは、メール送受信用のケーブル43、44のみで接続されていることが望ましい。こうすれば、サーバ3とメール転送部40との間でのデータ転送は、一定のメール形式以外で行われることがない。例えば、このメールで転送されるデータをテキストデータに限るようにすれば、不正なコマンドやプログラムがサーバ3とメール転送部40との間で転送されることが無い。

以上のシステムは次のように動作する。

サーバ3の記憶装置33には、例えばインターネット等のネットワーク1を通じて商品を販売するためのホームページ等のウェブページデータが格納されている。メールクライアント31は、端末装置2のユーザ等からネットワークを通じて商品発注のためのデータを受信すると、これをメール形式でメール転送部40のメール受信部41に送信する。メール受信部41は、受信したメールを受信データ記憶手段6に記憶させる。

その後の処理は既に説明したとおりで、データ形式の変換を経て、データベース9にそのデータが取り込まれる。データ変換部50は、データの形式をデータベース形式に変換して直接データベース9に書き込むような手段で構成してもよい。

一方、受注があった場合には、ホストコンピュータが「受信しました」といったコメントや、出荷日等を含む納期情報を生成する。このコメントや情報は、送信データ記憶手段12に記憶される。メール送信部42は、このコメントや情報をメール形式のデータにしてメールサーバ32に送信する。メールサーバ32は、そのデータをネットワークに向けて送信する。

即ち、メールクライアント31は、メール受信部41にメール形式のデータを送信するが、逆方向にメールを受信する機能は持たない。メールサーバ32はメール送信部42からメールを受信するが逆方向にメールを送信する機能は持たない。サーバ3とメール転送部40の間はメールを転送専用の通信回線等で接続されることが好ましい。こうして、サーバ3とメール転送部40とは、ハードウェア上も別体で構成できる。通信回線は、よりセキュリティを高めるために、他

のデータの侵入経路を持たないものであることが好ましい。またメール形式のデータであって、他の形式のデータを転送しないから、不正なコマンドやデータがホストコンピュータ側に取り込まれることが無い。従って、確実な一方通行のデータ転送路となる。これにより、高いセキュリティが要求されるシステムについて高い保護機能が発揮される。

図6は、メール転送を利用してセキュリティを強化した別のシステムのブロック図である。

この図の例では、システム20のウェブサーバ51がネットワーク1に接続されて、ネットワーク1との通信を行う。このウェブサーバ51はメールサーバ52と接続されている。メールサーバ52は、メール転送部40のメール受信部41とメール専用線53を介して接続されている。また、メールサーバ52は、メール転送部40のメール送信部42とメール専用線54を介して接続されている。この図のメール転送部40以下ホストコンピュータまでの部分は、図5と同一である。なお、メール転送部40が直接ホストコンピュータ10に接続されていても、また、メール転送部40がホストコンピュータ10の一部に組み込まれていても、このシステムは十分に高いセキュリティが確保できる。

上記メール専用線53、54は、メールサーバ52とメール転送部40との間のメール転送にのみ使用される。メール転送以外に使用しないので、限られたフォーマットのデータ以外を転送することが出来ない。従って、ネットワーク側からホストコンピュータ側への不法侵入が確実に阻止される。また、ホストコンピュータ側からネットワーク側へ不用意にデータが送り出されることが無い。なお専用線53、54は図のように上りと下りで別々のケーブルにより構成してもよいし、双方向転送が可能な1本のケーブルにより構成しても構わない。また、この具体例では、上記の説明の都合上、ネットワーク1からウェブサーバ51の方向にのみデータが転送されるように矢印を示したが、ネットワーク1とウェブサーバ51間は双方向のコミュニケーションをしてさしつかえない。

上記のシステムでは、端末装置2から商品発注のためのデータがネットワーク1に送信されると、ウェブサーバ51がこれを受信する。ウェブサーバ51は、受信したデータをメールサーバ52に送信する。メールサーバ52は、そのデー

タをメール形式で専用線 5 3 を介してメール受信部 4 1 に送信する。一方、ホストコンピュータ 1 0 から送信されるメールは、メール送信部 4 2 から専用線 5 4 を介してメールサーバ 5 2 に転送される。メールサーバ 5 2 は、自己のメール送信機能を使って、ネットワーク 1 を通じて端末装置 2 に向けて送信する。その他の部分は、これまで説明したものと同様のため、重複する説明を省略するが、このような、専用線 5 3、5 4 を使用したメール転送により、ネットワークからの内部システムの保護強化を図ることができる。

なお、各図に示した各機能ブロックは、それぞれ別々のプログラムモジュールにより構成してもよいし、一体化したプログラムモジュールにより構成してもよい。また、これらの機能ブロックの全部または一部を論理回路によるハードウェアで構成しても構わない。また、各プログラムモジュールは、既存のアプリケーションプログラムに組み込んで動作させてもよいし、独立のプログラムとして動作させてもよい。

[illegible]